

# Exhibit A

Yongmoon Kim (NJ Atty. ID #026122011)  
KIM LAW FIRM LLC  
411 Hackensack Avenue, Suite 701  
Hackensack, New Jersey 07601  
Telephone & Fax (201) 273-7117  
ykim@kimlf.com

*Attorneys for Plaintiff Carolina C. Zamora*

CAROLINA C. ZAMORA, *on behalf of herself  
and those similarly situated,*

Plaintiff,

vs.

MRS BPO, L.L.C.; and JOHN DOES 1 to 10,

Defendants.

SUPERIOR COURT OF NEW JERSEY  
LAW DIVISION: ESSEX COUNTY

Civil Action

Docket No.

**CLASS ACTION COMPLAINT  
and JURY DEMAND**

Plaintiff Carolina C. Zamora, individually and on behalf of those similarly situated, by way of Class Action Complaint against Defendant MRS BPO, L.L.C., and John Does 1 to 10, state:

#### **NATURE OF THE CASE**

1. This is a putative class action arising from Defendant, MRS BPO, L.L.C.'s unlawful disclosure of private financial information to third parties without the prior consent of the consumers.

2. The Fair Debt Collection Practices Act prohibits the disclosure of information to third parties to prevent identity theft and invasions of privacy. As the National Consumer Law Center put it eloquently:

As the world has gone digital, consumers' records, both financial and otherwise, are increasingly vulnerable to exposure. Transactions that were once fleeting, recorded only on paper and filed in some cabinet, or perhaps reduced to

microfiche, are now but mouse-clicks away from duplication and dissemination.

Unregulated databases, escalating numbers of mergers, and the proliferation of information brokers—private investigators who specialize in obtaining computerized records—all threaten privacy. As was noted in Congress, “databases of personal identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations.”

The internet raises particular privacy concerns, as information sent over the World Wide Web may pass through dozens of different computer systems, each of which can snatch and hold the information in its coffers. In addition, website owners can track consumers’ online behavior and gather information about their preferences, often without their knowledge. Web bugs, or tiny graphics that are put into web pages and e-mails, can monitor who views the information. Clickstream data can tell website owners which pages of the site were viewed and for how long. “Cookies” dropped onto a computer may not identify the user by name but do identify the particular computer, which allows an interested party to assemble a great deal of information about that computer’s user.

Financial information is especially sensitive, able to reveal not just a consumer’s standard of living and debt load, but also personal preferences and lifestyle details ranging from books bought to prescriptions purchased. In *California Bankers Ass’n v. Shultz*, Justice Powell pointed out that “[f]inancial transactions can reveal much about a person’s activities, associations, and beliefs.” Justice Douglas elaborated further:

A checking account . . . [m]ay well record a citizen’s activities, opinion, and beliefs as fully as transcripts of his telephone conversations . . . In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.

The same can be said of credit card charges, debit purchases, and online transactions. Forty years later, the details of these revealing consumer activities are easily collected, compiled, analyzed, and accessed, and thus have created a lucrative market for their trade. One industry leader among data aggregation companies, Acxiom, advertises that it has data on 2.5 billion consumers. Acxiom claims that one of its products covering American consumers has data on 250 million consumers, offering data not just on individual demographics, but also household characteristics, financial information, life events, major purchases, and behavior, all of which allows for targeted marketing. Experian reports that it manages data on more than 300 million consumers and 126 million households, while Equifax claims a database of over 115 million U.S. households distributed over 150 different segment groups, which can be used to predict behavior. In

2017, Equifax suffered a data breach that involved the personal data on nearly half the United States population being stolen, a breach that a Congressional committee found to have been “entirely preventable.” In 2014, the Federal Trade Commission filed a complaint against another data broker that allegedly bought the payday loan applications of consumers and then sold the information to marketers with no legitimate need for it, leading some scammers among them to debit millions from the consumers’ accounts.

National Consumer Law Center, Fair Credit Reporting (9th ed. 2017) § 18.1, *updated at* [www.nclc.org/library](http://www.nclc.org/library) (footnotes omitted and alterations in original) (attached as *Exhibit A*).

3. For example, in enacting the FDCPA, Congress found “abundant evidence of the use of abusive, deceptive, and unfair debt collection practices by many debt collectors. Abusive debt collection practices contribute to the number of personal bankruptcies, to marital instability, to the loss of jobs, and **to invasions of individual privacy**. 15 U.S.C. § 1692(a). *See also* *Douglass v. Convergent Outsourcing*, 765 F.3d 299, 303-04 (3d Cir. 2014) (“The disclosure of [the consumer’s] account number raises these privacy concerns. The account number is a core piece of information pertaining to [the consumer’s] status as a debtor and Convergent’s debt collection effort. Disclosed to the public, it could be used to expose her financial predicament. Because Convergent’s disclosure implicates core privacy concerns, it cannot be deemed benign.”).

4. Despite the *Douglass* ruling, Defendant continues to misuse and unlawfully disclose private financial information about consumers to third-parties.

5. Defendant’s disclosure of sensitive financial information to third parties is an act consistent with a course of conduct and practice which was either designed to, or had as its natural consequence, an attempt to obtain money from consumers through the use of false, misleading, deceptive, abusive, unfair, unconscionable, and unlawful conduct prohibited by common law and statutory law including, but not limited to, the Consumer Fraud Act (“CFA”),

N.J.S.A. 56:8-1, *et seq.*, and the Fair Debt Collection Practices Act (“FDCPA”), 15 U.S.C. §§ 1692, *et seq.*

6. Defendant is subject to strict liability under the FDCPA for the prohibited communication with third parties “without the prior consent of the consumer given directly to the debt collector . . . in connection with the collection of [the] debt, with any person other than the consumer . . . .” 15 U.S.C. § 1692c(b) and for violating 15 U.S.C. § 1692d(3).

7. Thus, Plaintiff bring this class action for damages against Defendant arising from Defendant’s unlawful disclosure of sensitive and confidential personal identifying and financial information, when attempting to collect debts from New Jersey consumers.

8. Defendant is subject to strict liability under the FDCPA for communicating with third parties “without the prior consent of the consumer given directly to the debt collector . . . in connection with the collection of [the] debt, with any person other than the consumer . . . .”

#### **JURISDICTION AND VENUE**

9. This Court has jurisdiction to entertain this matter pursuant to 15 U.S.C. § 1692k(d) and 28 U.S.C. § 1331.

10. Venue is proper in Essex County because Defendant regularly conducts business there, including the collection of debts against New Jersey residents residing in Essex County.

#### **PARTIES**

11. Plaintiff, Carolina C. Zamora (“Zamora”), is a natural person.

12. “Plaintiff” refers to Zamora.

13. At all times relevant to this lawsuit, Plaintiff was a citizen of the State of New Jersey.

14. Defendant, MRS BPO, L.L.C. (“Defendant” or “MRS”) is a collection agency with an office located at 1930 Olney Avenue, Cherry Hill, New Jersey 08003.

15. Defendants John Does 1 to 10 are natural persons and/or business entities all of whom reside or are located within the United States and personally created, instituted and, with knowledge that such practices were contrary to law, acted consistent with and oversaw policies and procedures used by the employees of Defendant that are the subject of this Complaint. Those defendants personally control the illegal acts, policies, and practices utilized by Defendant and, therefore, are personally liable for all of the wrongdoing alleged in this Complaint. Those fictitious names of individuals and businesses alleged for the purpose of substituting names of defendants whose identity will be disclosed in discovery and should be made parties to this action.

16. Some or all of John Does 1-10 set the policies and practices complained of herein.

17. Some or all of John Does 1-10 were actively engaged in the practices complained of herein.

18. In this pleading, “Defendants” in the plural refers to all Defendants.

#### **FACTUAL ALLEGATIONS**

##### **A. Allegations Regarding Defendant’s Practices Generally**

19. MRS regularly collects or attempts to collect debts that are past due.

20. MRS regularly collects or attempts to collect debts allegedly owed to others which were incurred primarily for personal, family or household purposes.

21. MRS is in the business of collecting debts or alleged debts of natural persons which arise from transactions which are primarily for personal, family, or household purposes.

22. The alleged receivables associated with the debts were assigned to MRS for the purpose of collection.

23. MRS uses the mail, telephone, the internet and other instruments of interstate commerce in engaging in the business of collecting defaulted debts or alleged debts of natural

persons which arise from transactions which are primarily for personal, family, or household purposes.

24. MRS is a collection agency.

**B. Plaintiff Zamora**

25. MRS has asserted that Zamora allegedly incurred or owed certain financial obligations arising out of a personal account.

26. The debt (“Debt”) arose from one or more transactions which were primarily for Zamora’s personal, family or household purposes.

27. This account (“Account”) was assigned to MRS for collection.

28. MRS contends that the Account is past due and in default.

29. The Account was past due and in default at the time it was placed with or assigned to MRS for collection.

30. In an attempt to collect the Debt, MRS mailed collection letters to Zamora on June 28, 2020 (“6/28/20 Letter”) and August 21, 2020 (“8/21/20 Letter”) to collect.

31. A true copy of the 6/28/20 Letter and 8/21/20 Letter but with redactions, is attached as ***Exhibit B***.

32. Zamora received and reviewed the MRS Letters.<sup>1</sup>

33. Upon information and belief, the MRS Letters were mailed using a third-party letter vendor.

34. Zamora never provided consent to Defendant to communicate to third parties regarding her Debt.

35. By using a letter vendor, Defendant has recklessly disclosed Zamora’s personal

---

<sup>1</sup> “MRS Letters” refers to the 6/28/20 Letter and 8/21/20 Letter.

identifying information and private information about her Debt to a third party without Zamora's prior consent.

36. Defendant unlawfully disclosed information about Zamora's Debt including the account numbers associated with the Debt and the alleged balances due.

37. The FDCPA prohibits a debt collector from communicating with third parties "without the prior consent of the consumer given directly to the debt collector . . . in connection with the collection of any debt, with any person other than the consumer, his attorney, a consumer reporting agency if otherwise permitted by law, the creditor, the attorney of the creditor, or the attorney of the debt collector ."<sup>2</sup>

38. The FDCPA also prohibits "[t]he publication of a list of consumers who allegedly refuse to pay debts . . . ."<sup>3</sup>

39. Unlawfully communicating with a third party letter vendor regarding Plaintiff's debts violates the FDCPA because it is impermissible communication under sections 1692c(b) and 1692d(3) which has the potential to cause harm to a consumer.<sup>4</sup>

40. MRS used the same procedures it used in sending the MRS Letters to Plaintiff when sending the same and/or similar letters to numerous other New Jersey consumers.

41. During the proposed class period, MRS sent letters the same or similar to the MRS Letters to numerous New Jersey consumers in an attempt to collect a debt.

42. It is MRS's policy and practice to unlawfully communicate and convey private and sensitive information about consumers with third parties by using third party vendors to send

---

<sup>2</sup> 15 U.S.C. § 1692c(b).

<sup>3</sup> 15 U.S.C. § 1692d(3).

<sup>4</sup> See *Hunstein v. Preferred Collection & Mgmt. Servs.*, 994 F.3d 1341 (11th Cir. 2021) (communicating with third party letter vendor violated the FDCPA).



written collection communications in attempts to collect consumer debts.

43. Upon information and belief, MRS published a list of debtors, including Plaintiff, that allegedly refuse to pay debts.

#### **CLASS ACTION ALLEGATIONS**

44. Plaintiff brings this action individually and as a class action on behalf of all others similarly situated pursuant to Rule 4:32 of the New Jersey Rules of Court.

45. Subject to discovery and further investigation which may require Plaintiff to modify the following class definition at the time Plaintiff moves for class certification, Plaintiff seeks certification of a class initially defined as follows:

**Class:** All natural persons residing in the State of New Jersey whose information was disclosed by Defendant to a third party on or after June 25, 2015, in an attempt to collect a Synchrony Bank account.

**FDCPA Subclass:** All natural persons residing in the State of New Jersey, to whom Defendant sent a collection letter; which letter (a) was dated within one year prior to June 25, 2021; (b) was seeking to collect a consumer debt allegedly owed to Synchrony Bank; and (c) was sent using a third party letter vendor.

46. Plaintiff seeks to recover statutory damages, actual damages, and attorney's fees and costs on behalf of herself and all class members under the claims asserted herein.

47. The Class for whose benefit this action is brought is so numerous that joinder of all members is impracticable.

48. There are questions of law and fact common to the members of the Class that predominate over questions affecting only individuals.

49. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. A class action will cause an orderly and expeditious administration of the claims of the Class and will foster

economies of time, effort and expense by avoiding thousands of individual suits that will be based on the same legal theories that can be resolved in a single proceeding.

50. Plaintiff's claim is typical of the claims of the members of the Class. She is a member of the Class.

51. The questions of law and/or fact common to the members of the Class predominate over any questions affecting only individual members.

52. Plaintiff does not have interests antagonistic to those of the Class.

53. The Class, of which Plaintiff is a member, are readily identifiable. The Defendant has records of each account.

54. Plaintiff will fairly and adequately protect the interests of the Class, and have retained competent counsel experienced in the prosecution of consumer litigation. Proposed Class Counsel have investigated and identified potential claims in the action; have a great deal of experience in handling class actions, other complex litigation, and claims of the type asserted in this action.

55. The prosecution of separate actions by individual members of the Class would run the risk of inconsistent or varying adjudications, which would establish incompatible standards of conduct for the Defendant in this action or the prosecution of separate actions by individual members of the class would create the risk that adjudications with respect to individual members of the class would as a practical matter be dispositive of the interests of the other members not parties to the adjudications or substantially impair or impede their ability to protect their interests. Prosecution as a class action will eliminate the possibility of repetitious litigation.

56. Plaintiff does not anticipate any difficulty in the management of this litigation.

**FIRST COUNT**  
**DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF FOR THE CLASS**

57. Plaintiff repeats and realleges all prior allegations as if set forth at length herein.

58. Defendant's prohibited disclosure of private and sensitive information constitute unfair and unconscionable commercial practices and otherwise violate the Consumer Fraud Act ("CFA") at N.J.S.A. 56:8-2 and the FDCPA at 15 U.S.C. § 1692 *et seq.*

59. Plaintiff suffered ascertainable loss from Defendant's CFA violations.

60. Plaintiff therefore has standing to seek injunctive and other equitable relief under the CFA, at N.J.S.A. 56:8-19, and the FDCPA.

61. Moreover, under the Uniform Declaratory Judgments Law at N.J.S.A. 2A:16-53, the Plaintiff and the putative Class members can seek declaratory relief.

62. The Defendant and its agents or others acting on their behalf should be enjoined from any further action or failing to take actions that result in any invasion of privacy, retain benefits from its illegal acts by the use of protected private and financial information.

**WHEREFORE**, as to Count One, Plaintiff, on behalf of herself and the putative class members, hereby requests a Judgment against Defendant, jointly and severally,

a. Granting class certification for class-wide equitable relief under R. 4:32-1(b)(2), and issuing a declaratory judgment applicable to the Plaintiff and putative Class and Subclass, pursuant to the Uniform Declaratory Judgments Law at N.J.S.A. 2A:16-53, ruling that:

1. Defendant violated the CFA.

2. Defendant violated the FDCPA.

b. Granting a permanent injunction against the Defendant, pursuant to the CFA, at N.J.S.A. 56:8-19, and the FDCPA prohibiting them from the disclosure of consumer's

information;

- c. Directing the Defendant to provide equitable notice relief pursuant to the CFA and FDCPA, providing for notice to Class members of the declaratory and injunctive ruling.
- d. Awarding Plaintiff's counsel reasonable attorneys' fees and costs under the CFA;
- e. For such other and further relief as the Court deems equitable and just.

**SECOND COUNT**  
**DAMAGES UNDER THE CONSUMER FRAUD ACT ON BEHALF OF THE CLASS**

63. Plaintiff repeats and realleges all prior allegations as if set forth at length herein.

64. Defendant is a "person" within the meaning of the CFA at N.J.S.A. 56:8-1.

65. Plaintiff and those similarly situated obtained "merchandise" within the meaning of the CFA at N.J.S.A. 56:8-1.

66. Defendant engaged in unconscionable commercial practices, deception, fraud, false promises, false pretenses and/or misrepresentations in connection with the sale of merchandise in violation of the CFA at N.J.S.A. 56:8-2.

67. Defendant engaged in unconscionable commercial practices, deception, fraud, false promises, false pretenses and/or misrepresentations in the subsequent performance of the sale of merchandise in violation of the CFA at N.J.S.A. 56:8-2.

68. Defendant committed unconscionable commercial practices, deception, fraud, false promises, false pretenses and/or misrepresentations in direct violation of the CFA at N.J.S.A. 56:8-2.

69. As a result of Defendant's unlawful actions, Plaintiff and the Class members suffered ascertainable loss from Defendant's CFA violations, entitling them to treble damages under the CFA, at N.J.S.A. 56:8-19.

**WHEREFORE**, as to Count Two, Plaintiff, on behalf of herself and the putative Class

members, hereby requests a Judgment against Defendant,

- a. Granting class certification of the Subclass under R. 4:32-1(b)(3);
- b. Awarding treble damages under the CFA, at N.J.S.A. 56:8-19;
- c. Alternatively awarding a refund of all moneys collected under the CFA, at N.J.S.A. 56:8-2.11;
- d. Awarding Plaintiff's counsel reasonable attorneys' fees and costs under the CFA, at N.J.S.A. 56:8-19;
- e. For pre-judgment and post-judgment interest; and
- f. For such other and further relief as the Court deems equitable and just.

**THIRD COUNT**  
**NEGLIGENCE ON BEHALF OF THE CLASS**

70. Plaintiff repeats and realleges all prior allegations as if set forth at length herein.

71. Defendant owed the Plaintiff a duty to maintain the confidentiality of their private and financial information.

72. Expert testimony is not required to establish that the disclosure of confidential and protected information breaches a commonly known duty owed by Defendant.

73. The disclosure of the confidential and protected information of the Plaintiff and the Class damaged them by exposing their private information to persons who lacked any right or entitlement to know their private information.

74. The Plaintiff and others have suffered a compensable loss arising from the disclosure of their protected private and financial information.

75. The Class has likewise suffered a compensable loss arising from the disclosure of their protected private and financial information.

**WHEREFORE**, as to Count Three, Plaintiff, on behalf of herself and the putative Class

members, hereby requests a Judgment against Defendant,

- a. Granting class certification of the Class under R. 4:32-1(b)(3);
- b. A money judgment for compensatory damages based on the Defendant's disclosure of the Plaintiff and Class' private information;
- c. For attorney's fees, litigation expenses and costs in connection with this action;
- d. For pre-judgment and post-judgment interest; and
- e. For such other and further relief as the Court deems equitable and just.

**FOURTH COUNT  
INVASION OF PRIVACY ON BEHALF OF THE CLASS**

76. Plaintiff repeats and realleges all prior allegations as if set forth at length herein.

77. Defendant invaded the privacy of Plaintiff by unreasonable publication of private facts.

78. These private facts, Plaintiff's financial information, are actually private matters, the dissemination of such facts would be offensive to a reasonable person and there is no legitimate interest of the public in being apprised of the facts publicized.

79. Expert testimony is not required to establish that the disclosure of confidential financial information invaded a person's privacy.

80. By publishing the private financial information of the Plaintiff and the Class, Defendant damaged them by exposing their private information to persons who lacked any right or entitlement to know their private financial information.

81. The Plaintiff and others have suffered a compensable loss arising from the invasion of their privacy.

82. The Class has likewise suffered a compensable loss arising from the invasion of their privacy.

**WHEREFORE**, as to Count Four, Plaintiff, on behalf of herself and the putative Class members, hereby requests a Judgment against Defendant,

- a. Granting class certification of the Class under R. 4:32-1(b)(3);
- b. A money judgment for compensatory damages based on the Defendant's invasion of the privacy of the Plaintiff and Class;
- c. For attorney's fees, litigation expenses and costs in connection with this action;
- d. For pre-judgment and post-judgment interest; and
- e. For such other and further relief as the Court deems equitable and just.

**COUNT FIVE**

**FAIR DEBT COLLECTION PRACTICES ACT FOR THE FDCPA SUBCLASS**

- 83. Plaintiff repeats and realleges all prior allegations as if set forth at length herein.
- 84. Defendant is a "debt collector" within the meaning of 15 U.S.C. § 1692a(6).
- 85. The Debt is a "debt" within the meaning of 15 U.S.C. § 1692a(5).
- 86. Plaintiff is a "consumer" within the meaning of 15 U.S.C. § 1692a(3).
- 87. The MRS Letters are "communication[s]" as defined by 15 U.S.C. § 1692a(2).
- 88. Defendant sent the MRS Letters in an attempt to collect a "debt" within the meaning of 15 U.S.C. § 1692a(5).
- 89. Defendant violated the FDCPA including sections 1692c, 1692c(b), 1692d, 1692d(3), and 1692f of the FDCPA.
- 90. Based on any one of those violations, Defendant is liable to Plaintiff and the Class for statutory damages, attorney's fees and costs under 15 U.S.C. § 1692k.

**WHEREFORE**, as to Count Five, Plaintiff, on behalf of herself and the putative Class members, hereby requests a Judgment against Defendant, MRS BPO, L.L.C.,

- a. An order certifying that the Cause of Action may be maintained as a class pursuant to R. 4:32 including defining the class, defining the class claims, and

appointing Plaintiff as the class representative and the undersigned attorney as class counsel;

- b. An award of statutory damages for Plaintiff pursuant to 15 U.S.C. § 1692k(a)(2)(A) and § 1692k(a)(2)(B)(i);
- c. An award of statutory damages for the Class pursuant to 15 U.S.C. § 1692k(a)(2)(B)(ii);
- d. Attorney's fees, litigation expenses, and costs pursuant to 15 U.S.C. § 1692k(a)(B)(3); and
- e. For pre-judgment and post-judgment interest; and
- f. For such other and further relief as may be just and proper.

#### **JURY DEMAND**

Plaintiff demands a trial by jury on all issues subject to trial by jury.

#### **DESIGNATION OF TRIAL COUNSEL**

Pursuant to Rule 4:25-4, Yongmoon Kim is designated as trial counsel for Plaintiff.

#### **CERTIFICATION**

Pursuant to Rule 4:5-1, I hereby certify to the best of my knowledge that the matter in controversy is not the subject of any action pending in any court or the subject of a pending arbitration proceeding, nor is any other action or arbitration proceeding contemplated. There are similar cases styled: *Scibilia v. MRS BPO, L.L.C.*, 2:21-cv-12684-JMV-JBC (D.N.J.) and *Liebman v. MRS BPO, L.L.C., et al.*, ESX-L-4578-21. I further certify that I know of no party who should be joined in this action at this time.

I hereby certify that pursuant to Rule 1:38-7: All confidential identifiers of the parties to this action have been redacted from all documents or pleadings submitted to the Court.



Dated: June 25, 2021

KIM LAW FIRM LLC

/s/ Yongmoon Kim  
Yongmoon Kim, Esq.

*Attorneys for Plaintiff*

The Fair Credit Reporting Act (FCRA) protects a limited segment of financial privacy, by regulating consumer reporting agencies (CRAs) that collect credit information about consumers, those who provide information to the CRAs, and those who seek information from CRAs. However, many consumer financial transactions do not fall within the FCRA, and other sources of privacy law must be examined to see if they can protect personal financial data from those who seek to acquire and exploit it. Discussed below are some federal statutes, state statutes, common law tort claims, and identity theft laws that may serve to shield consumers' economic conduct.

As the world has gone digital, consumers' records, both financial and otherwise, are increasingly vulnerable to exposure. Transactions that were once fleeting, recorded only on paper and filed in some cabinet, or perhaps reduced to microfiche, are now but mouse-clicks away from duplication and dissemination.

Unregulated databases, escalating numbers of mergers, and the proliferation of information brokers—private investigators who specialize in obtaining computerized records—all threaten privacy. As was noted in Congress, “databases of personal identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations.”<sup>1</sup>

The internet raises particular privacy concerns, as information sent over the World Wide Web may pass through dozens of different computer systems, each of which can snatch and hold the information in its coffers. In addition, website owners can track consumers' online behavior and gather information about their preferences, often without their knowledge. Web bugs, or tiny graphics that are put into web pages and e-mails, can monitor who views the information. Clickstream data can tell website owners which pages of the site were viewed and for how long. “Cookies” dropped onto a computer may not identify the user by name but do identify the particular computer, which allows an interested party to assemble a great deal of information about that computer's user.<sup>2</sup>

Financial information is especially sensitive, able to reveal not just a consumer's standard of living and debt load, but also personal preferences and lifestyle details ranging from books bought to prescriptions purchased. In *California Bankers Ass'n v. Shultz*,<sup>3</sup> Justice Powell pointed out that “[f]inancial transactions can reveal much about a person's activities, associations, and beliefs.” Justice Douglas elaborated further:

A checking account . . . [m]ay well record a citizen's activities, opinion, and beliefs as fully as transcripts of his telephone conversations . . . In a sense a person is defined by the checks he writes. By examining them the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum.<sup>4</sup>

The same can be said of credit card charges, debit purchases, and online transactions. Forty years later, the details of these revealing consumer activities are easily collected, compiled, analyzed, and accessed, and thus have created a lucrative market for their trade. One industry leader among data aggregation companies, Acxiom, advertises that it has data on 2.5 billion consumers.<sup>5</sup> Acxiom claims that one of its products covering American consumers has data on 250 million consumers, offering data not just on individual demographics, but also household characteristics, financial information, life events, major purchases, and behavior, all of which allows for targeted marketing.<sup>6</sup> Experian reports that it manages data on more than 300 million consumers and 126 million households,<sup>7</sup> while Equifax claims a database of over 115 million U.S. households distributed over 150 different segment groups, which can be used to predict behavior.<sup>8</sup> In 2017, Equifax suffered a data breach that involved the personal data on nearly half the United States population being stolen, a breach that a Congressional committee found to have been “entirely preventable.”<sup>9</sup> In 2014, the Federal Trade Commission filed a complaint against another data broker that allegedly bought the payday loan applications of consumers and then sold the information to marketers with no legitimate need for it, leading some scammers among them to debit millions from the consumers' accounts.<sup>10</sup>

Marketers are intensely interested in consumers' online and other behavior so they can pinpoint consumers for advertising.<sup>11</sup> Businesses want to learn as much about consumers as possible.<sup>12</sup> Furthermore, since the 9/11 attacks, the federal government, specifically the National Security Agency, has voraciously sought data about individuals both inside and outside the United States.<sup>13</sup> Political groups seek out and aggregate information about consumers to assign them “persuasion scores” that purport to measure how likely that consumer is to vote for or against a particular candidate.<sup>14</sup> Even the mundane task of grocery shopping is considered sufficiently informative that supermarkets use “loyalty cards” to track every item purchased by every cardholder, and they are free to sell that information to anyone who might be interested. There is a near insatiable hunger to

[EXHIBIT A]

learn how consumers get and spend their money.

Notwithstanding the sensitivity embedded in a person's financial choices, they are, for the most part, fair game for trade. While federal law protects against disclosure of video rental preferences,<sup>15</sup> cable viewing preferences,<sup>16</sup> medical records,<sup>17</sup> and student records,<sup>18</sup> it does not yet prevent financial or other institutions from selling their customers' Social Security numbers, account balances, maturity dates, securities holdings, or other information to private entities.<sup>19</sup> Consequently, consumers remain largely ignorant of the trafficking in such personal information.

In 2014, the FTC conducted an in-depth study of nine data brokers that collect personal information about consumers and then sell it for marketing and other purposes, and issued an extensive and often critical report.<sup>20</sup> In addition to describing the processes by which data brokers gather and use consumer information, the agency called for Congress to "consider enacting legislation that would enable consumers to learn of the existence and activities of data brokers and provide consumers with reasonable access to information about them held by these entities."<sup>21</sup> In effect, this is a call for Congress to extend some of the basic rights provided by the FCRA to data that falls outside that act. However, there could be downsides to such legislation to regulate data brokers, such as preemption of stronger state laws and potential impairment of the FCRA if brokers are covered under both that Act and the proposed law.

Though the FCRA limits some disclosures by private parties of consumer financial information, it does not give consumers the right to prohibit a CRA from disclosing accurate, nonobsolete information to those deemed to have a permissible purpose.<sup>22</sup> Furthermore, while some data warehouses fall within the definition of a CRA,<sup>23</sup> others that sell their records for reasons other than those included in the definition of a CRA may evade the FCRA's restrictions.<sup>24</sup>

In addition, the Gramm-Leach-Bliley Act (the GLBA) gives consumers a limited right to "opt out" of certain disclosures by financial institutions to nonaffiliated third parties.<sup>25</sup> However, its abundant exceptions arguably all but destroy the protection it purports to provide.

American privacy law is poorly suited to protecting privacy, especially of computerized consumer information. Aside from the FCRA, privacy laws largely fall into three categories: laws protecting personal privacy from invasions by governments, federal or local; the common law tort of invasion of privacy; and statutes and case law that prohibit private parties from obtaining<sup>26</sup> or disclosing<sup>27</sup> specific types of information. Relevant provisions of the GLBA<sup>28</sup> will be described in this last category;<sup>29</sup> they impose certain notice requirements on financial institutions who disclose financial data and a limited right for consumers to opt out of some kinds of disclosures.

## Footnotes

1 {1} Personal Data Privacy and Security Act of 2005, S. 1332, 109th Cong. (June 29, 2005).

2 {2} See [www.epic.org/privacy/internet/cookies](http://www.epic.org/privacy/internet/cookies) [1].

3 {3} 416 U.S. 21 (1974).

4 {4} *Id.* at 85, 90 (Douglas, J., dissenting).

5 [Acxiom Data: Unparalleled Global Consumer Insights](https://www.acxiom.com) [2] 2, available at <https://www.acxiom.com>.

6 [Acxiom Data: Unparalleled Global Consumer Insights](https://www.acxiom.com) [2] 3–4, available at <https://www.acxiom.com>.

7 {7} [Experian. Experian Marketing Services: Consumer View](https://www.experian.com) [3], available at <https://www.experian.com>.

- 8 {8} [Equifax, Compiled Data](#) [4], *available at* [www.equifax.com](http://www.equifax.com). In 2017, Equifax had credit information on 820 million consumers. U.S. House of Representatives, Committee on Oversight and Government Reform Majority Staff Report, [The Equifax Data Breach](#) [5] 15 (Dec. 2018), *available at* <https://republicans-oversight.house.gov>.
- 9 U.S. House of Representatives, Committee on Oversight and Government Reform Majority Staff Report, [The Equifax Data Breach](#) [5] 2 (Dec. 2018), *available at* <https://republicans-oversight.house.gov>.
- 10 {10} [Fed. Trade Comm'n, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts \(Dec. 23, 2014\)](#) [6], *available at* [www.ftc.gov](http://www.ftc.gov).
- 11 {11} *See* Frank Pasquale, *The Dark Market for Personal Data*, N.Y. Times, Oct. 16, 2014.
- 12 {12} *See, e.g.*, Stephanie Clifford and Quentin Hardy, *Attention, Shoppers: Store Is Tracking Your Cell*, N.Y. Times, July 14, 2013; Your Privacy for Sale, Consumer Rep. (Oct. 2006).
- 13 {13} *See* [James Risen and Laura Poitras, N.S.A. Gathers Data on Social Connections of U.S. Citizens, N.Y. Times, Sept. 28, 2013](#) [7], *available at* [www.nytimes.com](http://www.nytimes.com) (describing the practices of NSA in analyzing phone call and e-mail logs, along with material from “public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information,” for both foreigners and Americans alike).
- 14 {14} For instance, in the 2016 election the data analytics company Cambridge Analytica claimed to have developed “psychographic” profiles on potential voters that the Trump campaign could exploit to grow its voter base. *See* Nicholas Confessore and Danny Hakim, *Data Firm Says “Secret Sauce” Aided Trump; Many Scoff*, N.Y. Times, Mar. 6, 2017, at A1. *See also* Jim Rutenberg, *Data You Can Believe In: The Obama Campaign’s Digital Masterminds Cash In*, N.Y. Times Magazine, June 20, 2013. One data-mining company that specializes in voter information, Aristotle, Inc., advertises that it maintains a “massive and ever-expanding database [that] includes over 190 million U.S. voters” and that it can “microtarget[]” individuals based on their “interests and hobbies,” along with “political district, political party affiliation, super-voters, gender, ethnicity, marital status, wealth, educational level and presence of children.” <http://aristotle.com/political-data> [8].
- 15 {15} Video Privacy Protection Act of 1988, 18 U.S.C. § 2710.
- Several states have similar acts, some of which extend beyond prohibiting merely the disclosure of video rental records to the disclosure of the purchase or rental of *any* written materials. *See, e.g.*, Mich. Comp. Laws § 445.1712 (known as both Michigan’s Preservation of Privacy Act and the Video Rental Privacy Act) (prohibiting, with exceptions anyone who is “engaged in the business of selling at retail . . . written materials” from disclosing information about the transaction in a way that “indicates the identity of the customer”). *See also* Coulter-Owens v. Rodale, Inc., 2015 WL 575004, at \*4 (E.D. Mich. Feb. 11, 2015) (denying dismissal of claim under state video rental privacy act arising from the alleged sale by the defendant, a magazine publisher, of subscribers’ information to data-mining companies). The Sixth Circuit recently limited the reach of Michigan’s act by concluding that a magazine publisher that used independent third parties to sell subscriptions could not be liable to a customer who had bought a subscription to its publication because the publisher was therefore not “in the business of selling at retail.” Coulter-Owens v. Time Inc., 695 Fed. Appx. 117, 123–124 (6th Cir. 2017).
- 16 {16} Cable Communications Policy Act of 1984, 47 U.S.C. § 551(c). Note that the USA PATRIOT Act expanded the list of disclosures permitted by the Cable Communications Policy Act by adding certain disclosures made to specified government authorities. Pub. L. No. 107-56, § 211 (Oct. 26, 2001), *amending* 47 U.S.C. § 551(c).

17 {17} Most health insurers and providers must comply with the Privacy Rule promulgated pursuant to the Health Insurance Portability and Accountability Act (HIPAA). 45 C.F.R. §§ 160.101 to 160.312, §§ 164.102 to 164.534. The HIPAA Privacy Rule generally prohibits covered entities from using or disclosing protected health information except as specifically allowed. Among the permitted disclosures are those to CRAs for purposes of payment, so long as the disclosure is limited to the following information: name and address, date of birth, Social Security number, payment history, account number, and name and address of the health care provider. 45 C.F.R. §§ 164.501, 164.506(c)(1). In 2009, Congress expanded the categories of those subject to HIPAA's anti-disclosure requirements in the Health Information Technology for Economic and Clinical Health Act (the HITECH Act). Pub. L. No. 111-5, 123 Stat. 115 (Feb. 7, 2009) (codified in scattered sections of titles 26 and 42 of the United States Code). *See also* 45 C.F.R. § 160.103 (containing an expanded definition of the "business associates" who are subject to the anti-disclosure provisions). For a discussion of the HIPAA Privacy Rule, see National Consumer Law Center, [Collection Actions § 9.3.4](#) [9] (4th ed. 2017), *updated at* [www.nclc.org/library](http://www.nclc.org/library). *See* [§ 5.4](#) [10], *supra*, for a discussion of the FCRA's restrictions on medical information.

18 {18} Family Educational Rights & Privacy Act of 1974, 20 U.S.C. § 1232g.

19 {19} Federal law prohibits firms and persons who regularly prepare income tax returns for others from disclosing personal tax information or using it for other purposes, with a few exceptions. 26 U.S.C. § 7216. The Privacy Act of 1974, 5 U.S.C. § 552a, requires all government agencies, whether federal, state, or local, that request Social Security numbers to provide a disclosure statement that explains whether the consumer is required to provide the number, how it will be used, and under what statutory authority the agency is requesting the number. The Act provides that a consumer cannot be denied a benefit for refusing to provide the number unless the number is required by federal law (or the disclosure is to an agency that had been using Social Security numbers prior to enactment of the Privacy Act). Although usually a consumer is not compelled to disclose her Social Security number to a private business, no federal law prohibits them from asking for it or from refusing to do business with a consumer who refuses to provide it.

20 {20} [Fed. Trade Comm'n, Data Brokers: A Call for Transparency and Accountability, at i \(May 2014\)](#) [11], *available at* [www.ftc.gov](http://www.ftc.gov).

21 {21} *Id.* at vii. The FTC noted these specific concerns: "Data brokers acquire a vast array of detailed and specific information about consumers; analyze it to make inferences about consumers, some of which may be considered sensitive; and share the information with clients in a range of industries. *All of this activity takes place behind the scenes, without consumers' knowledge.*" *Id.* (emphasis added).

22 {22} The Act additionally imposes some restrictions on users of consumer reports and imposes obligations on those that furnish information to CRAs to provide accurate information. *See* [Chs. 6](#) [12] and [7](#) [13], *supra*. Some state laws give consumers the right to deny access to, or to "freeze," their consumer reports. *See* [§ 9.4.1](#) [14], *supra*, and [Appx. H](#) [15], *infra*.

23 {23} *See* [§ 2.7.5](#) [16], *supra*.

24 {24} U.S. Gov't Accountability Office, GAO-06-674, Report to the Committee on Banking, Housing and Urban Affairs, U.S. Senate: Personal Information: Key Federal Privacy Laws Do Not Require Information Resellers to Safeguard All Sensitive Data (June 2006). *See generally* [Ch. 2](#) [17], *supra* (discussing what constitutes a "consumer report" and "consumer reporting agency").

25 {25} *See* [§ 18.4.1](#) [18], *infra*.

26 {26} For example, through wiretapping. *See, e.g.*, 18 U.S.C. § 2510; Cal. Penal Code §§ 631 to 637; Conn. Gen. Stat. Ann. §§ 53a-187 to 53a-189b; Haw. Rev. Stat. § 711-1111.

[EXHIBIT A]

## 18.1 Introduction

27 {27} For example, the disclosure of customers' video recording rentals. *See, e.g.*, Cal. Civ. Code § 1799.3 (West); Conn. Gen. Stat. Ann. § 53-450; Iowa Code Ann. § 727.11.

28 {28} 15 U.S.C. §§ 6801 to 6810.

29 {29} *See* [§ 18.4.1](#) [18], *infra*.

**Source:** National Consumer Law Center, Fair Credit Reporting [9th ed.], updated at [www.nclc.org/library](http://www.nclc.org/library)

**Source URL:** <https://library.nclc.org/fcr/1801-0>

### Links

- [1] <http://www.epic.org/privacy/internet/cookies>
- [2] [https://www.acxiom.com/wp-content/uploads/2019/02/Acxiom\\_Data\\_Overview\\_2019\\_02.pdf](https://www.acxiom.com/wp-content/uploads/2019/02/Acxiom_Data_Overview_2019_02.pdf)
- [3] <https://www.experian.com/marketing-services/targeting/data-driven-marketing>
- [4] <http://www.equifax.com/compiled-data/>
- [5] <https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf>
- [6] <https://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars>
- [7] [http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?\\_r=0](http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0)
- [8] <http://aristotle.com/political-data>
- [9] <https://library.nclc.org/nclc/link/CA.09.03.04>
- [10] <https://library.nclc.org/nclc/link/FCR.05.04>
- [11] [https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf?utm\\_source=govdelivery](https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf?utm_source=govdelivery)
- [12] <https://library.nclc.org/nclc/link/FCR.06>
- [13] <https://library.nclc.org/nclc/link/FCR.07>
- [14] <https://library.nclc.org/nclc/link/FCR.09.04.01>
- [15] <https://library.nclc.org/nclc/link/FCR.AH>
- [16] <https://library.nclc.org/nclc/link/FCR.02.07.05>
- [17] <https://library.nclc.org/nclc/link/FCR.02>
- [18] <https://library.nclc.org/nclc/link/FCR.18.04.01>





S-SFMRSA11  
PCD7HU00511560 - 627098373 I23120  
Return Address :  
MRS BPO, L.L.C.  
1930 OLNEY AVENUE  
CHERRY HILL NJ 08003

1930 OLNEY AVENUE  
CHERRY HILL NJ 08003  
866-249-6063

Office Hours:  
Monday - Thursday 9am - 9pm ET  
Friday 9am - 5pm ET

REDACTED



CAROLINA ZAMORA

Redacted  
Redacted

June 28, 2020

MERCHANT: Redacted
CREDITOR: Redacted
MRS ACCT#: Redacted
CREDITOR ACCT#: xxx Redacted
ACCOUNT BALANCE: Redacted

Dear CAROLINA ZAMORA,

The above referenced creditor has placed your account with our office for collection.

Resolving a long overdue debt is never easy. We are ready to assist you to find a solution that is both fair and reasonable. Please reach out to us using any one of our convenient contact methods.



Pay via the Web  
<https://portal.mrsbpo.com>



Pay by Phone  
866-249-6063



Pay by Mail  
MRS BPO, LLC  
1930 Olney Avenue,  
Cherry Hill, NJ 08003

**IMPORTANT CONSUMER INFORMATION**

Unless you notify this office within 30 days after receiving this notice that you dispute the validity of the debt or any portion thereof, this office will assume this debt is valid. If you notify this office in writing within 30 days from receiving this notice that you dispute the validity of this debt or any portion thereof, this office will obtain verification of the debt or obtain a copy of a judgment and mail you a copy of such judgment or verification. If you request of this office in writing within 30 days after receiving this notice, this office will provide you with the name and address of the original creditor, if different from the current creditor.

Sincerely,

MRS BPO, L.L.C.  
866-249-6063

This is an attempt to collect a debt and any information obtained will be used for that purpose.  
This communication is from a debt collector.

[EXHIBIT B]



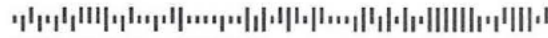
S-SFMRSA11  
PCNIYU00200567 - 633024129 I01134  
Return Address :  
MRS BPO, L.L.C.  
1930 OLNEY AVENUE  
CHERRY HILL NJ 08003



1930 OLNEY AVENUE  
CHERRY HILL NJ 08003  
844-289-4054

Office Hours:  
Monday - Thursday 9am - 9pm ET  
Friday 9am - 5pm ET

REDACTED



CAROLINA ZAMORA

Redacted  
Redacted

August 21, 2020

MERCHANT:	Redacted
CREDITOR:	Redacted
MRS ACCT#	Redacted
CREDITOR ACCT#:	xxxRedacted
ACCOUNT BALANCE:	Redacted

Dear CAROLINA ZAMORA,

We recognize that a possible hardship or pitfall may have prevented you from satisfying your obligation. MRS is here to work with you towards a resolution of the matter listed above. We have several options available to assist you with the resolution of your account, such as:

- Payment arrangement towards the full outstanding balance. The 1st payment would be received by 09/04/2020 and eleven (11) additional monthly payments received on the same day of each month thereafter until the balance is paid in full.
- Payment of an agreed upon discounted amount - Repayment of an amount that is less than the full outstanding balance of the account to resolve the matter.

Please contact us by using one of the methods listed below to resolve any of the above offer or for additional offers that may be available to you. We look forward to assisting you.



**Pay via the Web**  
<https://portal.mrsbpo.com>



**Pay by Phone**  
844-289-4054



**Pay by Mail**  
MRS BPO, LLC  
1930 Olney Avenue,  
Cherry Hill, NJ 08003

When you call please let our representative know that you have received the REDACTED Option Letter.

Sincerely,

MRS BPO, L.L.C.  
844-289-4054  
Letter ID: DU8.265575.1236887

This is an attempt to collect a debt and any information obtained will be used for that purpose.  
This communication is from a debt collector.

[EXHIBIT B]